

**IN THE UNITED STATES DISTRICT COURT  
FOR THE MIDDLE DISTRICT OF TENNESSEE**

**VIP PHYSICIANS CONSULTING LLC**  
individually and on behalf of all others  
similarly situated,

Plaintiff,

-v.-

**CHANGE HEALTHCARE INC.,  
OPTUM, INC., and UNITEDHEALTH  
GROUP INC.,**

Defendants.

Case No.

**CLASS ACTION COMPLAINT**

**JURY DEMAND**

Plaintiff VIP Physicians Consulting LLC (“Plaintiff”) brings this Class Action Complaint, individually and on behalf of all others similarly situated (the “Class Members”), against Defendants Change Healthcare, Inc. (“Change”), Optum, Inc. (“Optum”), and UnitedHealth Group, Inc. (“UHG”) (collectively, “Defendants”) alleging as follows, based upon information and belief, investigation of counsel, and personal knowledge.

**I. NATURE OF CASE**

1. Between February 12, 2024 and February 21, 2024, Change experienced a data breach and ransomware attack which exposed sensitive medical records and identifying information for up to 112 million United States patients, as well as billing, insurance, and other data. Change is a subsidiary of healthcare mega-conglomerate UHG, providing online administrative and technological support for payers, providers, and consumers. A little known but fundamental component of America’s healthcare infrastructure, Change performs more than one hundred critical functions used by over one million physical and mental healthcare providers,

including hospitals, physicians, therapists, pharmacies, dentists, and laboratories, processing an estimated 15 billion healthcare transactions annually.

2. Hackers gained access to Change's systems and the data therein by simply using compromised login credentials on an outward-facing web-based "portal" for employees. For approximately nine days, the hackers, undetected, proceeded to review the data in Change's internal systems, exploiting apparently unrestricted access to not only folders and files containing sensitive information from providers across the healthcare industry, but also source code files for Change's healthcare services. During that extended period, the hackers methodically exfiltrated volumes of information which they selected for maximum vulnerability, sensitivity, and value. While securing the data, the hackers also modified and compromised Change's internal systems, including Change's backup systems, to bring them under the hackers' own direct control.

3. The hackers, members of known cybercriminal organization ALPHV/BlackCat, were not detected by any security measure implemented by Defendants, even though they would have been detected, or even stopped at the door, if Defendants had implemented basic cybersecurity precautions that the FBI and other authorities specifically urged businesses to implement, no later than April 2022, to prevent and protect against data breach and ransomware attacks by this specific organization.

4. After nine days exploring and extracting some of the nation's most sensitive, valuable data, on or around February 21, 2024, the hackers finally announced their presence to Defendants by triggering software they had installed in their extended foray. It perpetrated a system-wide ransomware attack, which, consistent with the group's well-known reputation and guidance from the FBI, locked Defendants out of Change's internal systems. The lockout extended to Change's backup systems, which apparently were not kept in a secure offline location, but

instead were accessible via the same employee portal as other private data in Defendants' care. ALPHV/BlackCat then made demands to Defendants, threatening to sell the exfiltrated data on the dark web, and to continually block access to Change's systems, unless Defendants acceded to their demands and paid a ransom.

5. Defendants paid the ransom. In addition, lacking any reasonable incident response plan for this scenario, Defendants also disabled and disconnected Change's systems nationwide, ostensibly to (finally) prevent further encroachments. This action by Defendants halted insurance authorizations, billing, and payments for approximately one-third of healthcare transactions in the United States. For over a month, there was a total cessation of critical services. During the total shutdown, pre-existing claims that healthcare providers had submitted for payment went unpaid; to the extent new claims could be made, they went unprocessed; and numerous standard functions required to provide healthcare services, such as insurance pre-authorizations, could not be performed. Defendants began to restore certain services in late March 2024, but the process has been slow and is still ongoing to this day.

6. The impact of Defendants' decisions on hard-working medical providers around the country was catastrophic. The unavailability of Change's mission-critical services resulted in unpaid claims, overdue payments, interest accumulation, inability to perform eligibility verifications leading to loss of services, increased administrative costs caused by manual processes, negative credit impact, and other harms. According to some estimates, by mid-March, providers were losing between \$500 million and \$1 billion in revenue *daily* because of the shutdown. By late March, healthcare providers faced a backlog of over \$14 billion just in unpaid and unprocessed claims, severely impairing their ability to make payroll, order supplies, and otherwise fund their operations.

7. Defendants compounded problems for providers, and the healthcare industry in general, by withholding information and refusing to provide an accurate timeline for restoring Change's services, among many other shortcomings and failures. Upon learning that Change's backup systems had been compromised, Defendants knew and must have known that providers should turn to Defendants' competitors to maintain at least some of their normal operations. Defendants withheld that fact, instead suggesting to struggling providers, day after day, that services may be restored the next day. Even today, Defendants have not provided a conclusive date by which they intend to bring all provider accounts, and services, current.

8. Defendants, with basic industry standard cybersecurity, threat detection, and incident response measures, including measures recommended in response to the known tactics of ALPHV/BlackCat years prior, could have prevented the attack and events that followed. They chose instead to shift the brunt of the impact of their poor security and planning to healthcare providers, including Plaintiff. Accordingly, Plaintiff brings this action against Defendants seeking redress for their unlawful and tortious conduct and asserting claims for negligence and unjust enrichment. Through these claims, Plaintiff seeks damages in an amount to be proven at trial, as well as injunctive and other equitable relief, including improvements to Defendants' data security systems and incident response planning.

## **II. THE PARTIES**

9. Plaintiff VIP Physicians Consulting LLC is a resident of Broward County, Florida and maintains its principal place of business in Fort Lauderdale, Florida.

10. Defendant Change Healthcare Inc. is a corporation incorporated in Delaware with its principal place of business in Nashville, Tennessee. Change became a subsidiary of UnitedHealth Group Incorporated in 2022 and is operated by Optum, Inc., another UnitedHealth Group subsidiary.

11. Defendant Optum, Inc. is a corporation incorporated in Delaware with its principal place of business in Eden Prairie, Minnesota.

12. Defendant UnitedHealth Group Inc. is a Delaware corporation with its principal place of business in Minnetonka, Minnesota.

### **III. JURISDICTION AND VENUE**

13. This Court has original jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. §§ 1332(d) and 1367 because Plaintiff and at least one member of the putative Class, as defined below, are citizens of a different state than Defendants, there are more than 100 putative class members, and the amount in controversy exceeds \$5 million exclusive of interest and costs.

14. This Court may exercise jurisdiction over Defendants because they are registered to conduct business in Tennessee; have sufficient minimum contacts in Tennessee; and intentionally avail themselves of the markets within Tennessee through the promotion, sale, and marketing of their services, thus rendering the exercise of jurisdiction by this Court proper and necessary.

15. Venue is proper in this District under 28 U.S.C. § 1391 because Defendant Change Healthcare Inc. resides in this District and a substantial part of the events or omissions giving rise to Plaintiff's claims occurred in this District.

### **IV. BACKGROUND**

16. UHG is a healthcare mega-conglomerate. UHG operates two primary businesses, UnitedHealthcare and Optum. UnitedHealthcare provides healthcare benefits, including through partnerships with government programs such as Medicaid. Optum is a technology company that provides "health services," leveraging technology and data to provide clinical, administrative and financial processes for insurers, providers, and others throughout the healthcare industry.

17. Change, (known as Emdeon before rebranding in 2015), is a healthcare services company established in 2005. Among other services, Change operates “the nation’s largest electronic data interchange (EDI) clearinghouse, which transmits data between healthcare providers and insurers, allowing them to exchange insurance claims, remittances, and other healthcare-related transactions . . . .”<sup>1</sup>

18. UHG acquired Change in October 2022 for purposes of merging Change’s business with UHG’s Optum, announcing in a press release that, “[t]he combined businesses share a vision for achieving a simpler, more intelligent and adaptive health system for patients, payers and care providers. The combination will connect and simplify the core clinical, administrative and payment processes health care providers and payers depend on to serve patients. Increasing efficiency and reducing friction will benefit the entire health system, resulting in lower costs and a better experience for all stakeholders.”<sup>2</sup> According to the United States Department of Justice, which filed an ultimately unsuccessful suit to stop the transaction, UHG gained “over a decade’s worth of historic data as well as billions of new claims each year” through the merger.<sup>3</sup>

19. The scale of Change’s penetration and integration within the United States healthcare system is extensive. An estimated 50 percent of all medical claims in the United States pass through Change’s EDI clearinghouse. As shown in the illustration below,<sup>4</sup> EDI

---

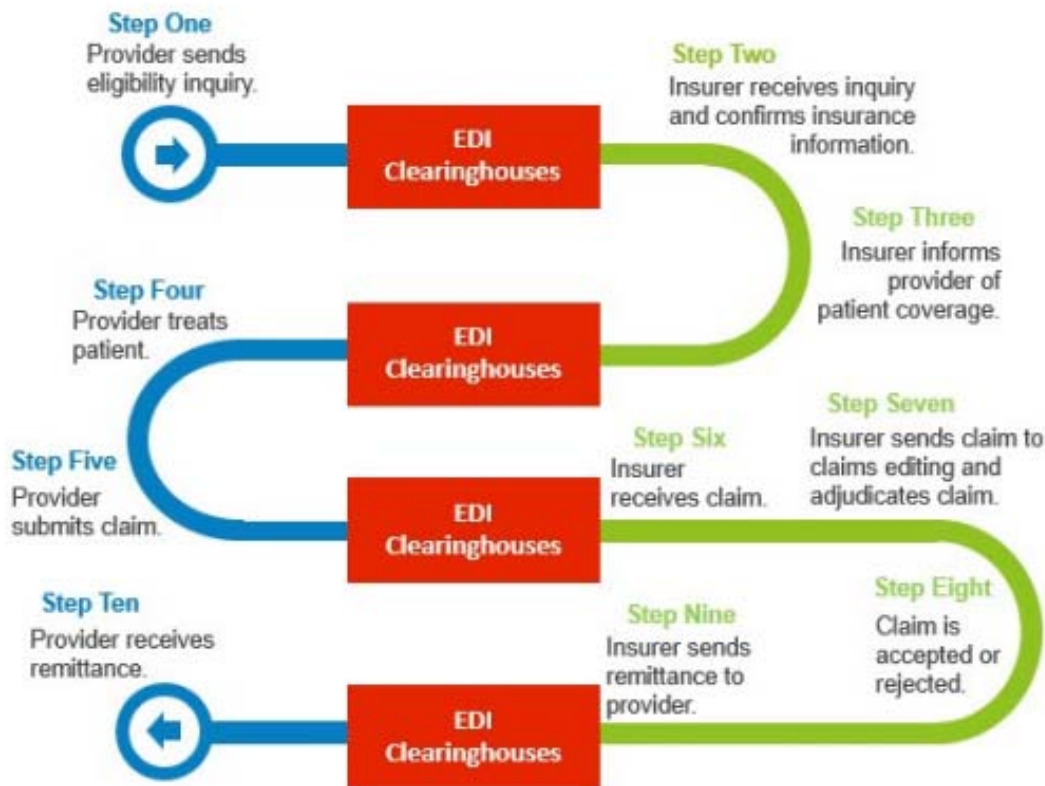
<sup>1</sup> See *United States et al. v. UnitedHealth Group, Inc. et al.*, No. 22-cv-00481 (Dkt. 1), <https://www.justice.gov/atr/case-document/file/1476901/dl> (Feb. 24, 2022).

<sup>2</sup> See Optum, *Optum and Change Healthcare Complete Combination* (October 22, 2022), <https://www.optum.com/en/about-us/news/page.hub.optum-and-change-healthcare-complete-combination.html>.

<sup>3</sup> See *United States et al. v. UnitedHealth Group, Inc. et al.*, No. 22-cv-00481 (Dkt. 1), <https://www.justice.gov/atr/case-document/file/1476901/dl> (Feb. 24, 2022).

<sup>4</sup> *Id.*

Clearinghouses such as Change's perform at least four crucial functions in the provision of patient care:



20. Change's "pervasive network connectivity," as Change described its business in its 2019 S-1 filing when the company went public, impacts "the vast majority of US payers and providers" because Change operates fundamental technological infrastructure connecting "approximately, 2,200 government and commercial payers" with 900,000 physicians, 118,000 dentists, 33,000 pharmacies, 5,500 hospitals, and 600 laboratories," and processes clinical records for over 112 million unique patients in the United States.<sup>5</sup> According to the company's website,

<sup>5</sup> See Form S-1 Registration Statement, Change Healthcare, Inc., <https://www.sec.gov/Archives/edgar/data/1756497/000119312519076886/d638353ds1.htm> (March 15, 2019).

Change processes 15 billion healthcare transactions each year, and its "clinical connectivity solutions" touch a third of U.S. patients.<sup>6</sup>

**A. The data breach and Ransomware Attack**

21. Hackers entered Change's systems on February 12, 2024 through an open door. According to UHG's Chief Executive Officer in his testimony before Congress on May 1, 2024, the hackers used login credentials for Change's outward-facing remote login application for employees (the "Change Healthcare Citrix portal"). Change's Citrix portal did not require users to complete multi-factor authentication, such as a one-time code sent to a personal device, or any other identity verification in order to log in.

22. For at least a week after the hackers first accessed Change's systems and databases, Defendants failed to detect their exploits. As UHG admits, they "moved laterally within the systems in more sophisticated ways and exfiltrated data."<sup>7</sup> They also installed software necessary to perpetrate their ransomware attack. On or around February 21, 2024, Defendants finally became aware Change's systems and data had been compromised when the hackers deployed ransomware to encrypt critical systems throughout Change's information technology environments, preventing UHG, Optum, and Change from accessing them.

23. On February 28, 2024, the cybercriminal organization ALPHV/BlackCat took responsibility for the attack. The group been in operation since November 2021 and its tactics are well-known among cybersecurity professionals.<sup>8</sup> Indeed, it has been the subject of numerous

---

<sup>6</sup> See <https://www.changehealthcare.com/> (last visited May 3, 2024).

<sup>7</sup> Testimony of Andrew Witty, Chief Executive Officer, UnitedHealth Group, Before the House Energy and Commerce Committee Subcommittee on Oversight and Investigations "Examining the Change Healthcare Cyberattack," [https://d1dth6e84htgma.cloudfront.net/Witty\\_Testimony\\_OI\\_Hearing\\_05\\_01\\_24\\_5ff52a2d11.pdf](https://d1dth6e84htgma.cloudfront.net/Witty_Testimony_OI_Hearing_05_01_24_5ff52a2d11.pdf) (May 1, 2024).

<sup>8</sup> See TrendMicro, *Ransomware Spotlight, BlackCat*, <https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-blackcat> (October 22, 2022).

advisories and warnings from government authorities. The FBI Cyber Division, for example, publicly issues “alerts” and “advisories” to help companies guard against ransomware. In April 2022, the FBI issued a detailed technical advisory about ALPHV/BlackCat, warning businesses that: (1) “BlackCat/ALPHV ransomware leverages previously compromised user credentials to gain initial access to the victim system;” (2) “Once the malware establishes access, it compromises Active Directory user and administrator accounts;” and (3) “BlackCat/ALPHV steals victim data prior to the execution of the ransomware, including from cloud providers where company or client data was stored.”<sup>9</sup> The FBI provided technical specifications concerning the characteristics of the group’s prior attacks, to facilitate identification of future attacks, and recommended measures to prevent future data breaches and ransomware attacks by ALPHV/BlackCat, urging businesses to:

- Use multifactor authentication where possible.
- Regularly change passwords to network systems and accounts, and avoid reusing passwords for different accounts.
- Disable unused remote access/Remote Desktop Protocol (RDP) ports and monitor remote access/RDP logs.
- Implement network segmentation.
- Audit user accounts with administrative privileges and configure access controls with least privilege in mind.
- Require administrator credentials to install software.
- Implement a recovery plan to maintain and retain multiple copies of sensitive or proprietary data and servers in a physically separate, segmented, secure location (e.g., hard drive, storage device, the cloud).
- Regularly back up data, air gap, and password protect backup copies offline. Ensure copies of critical data are not accessible for modification or deletion from the system where the data resides.<sup>10</sup>

---

<sup>9</sup> See FBI Cyber Division, *BlackCat/ALPHV Ransomware Indicators of Compromise*, <https://www.ic3.gov/Media/News/2022/220420.pdf> (Apr. 19, 2022).

<sup>10</sup> *Id.*

24. In the April 2022 advisory, the FBI also discouraged businesses that did experience a ransomware attack from paying a ransom, explaining that “[p]ayment does not guarantee files will be recovered. It may also embolden adversaries to target additional organizations, encourage other criminal actors to engage in the distribution of ransomware, and/or fund illicit activities.”<sup>11</sup> The data breach and ransomware attack here were consistent with the group’s widely-reported past operations and could have been prevented by implementing even some of the recommended measures above.

25. When ALPHV/BlackCat publicized the event on February 28, 2024 in a post on its dark web leak site, it announced that UHG had lied to the public about the nature and extent of the data breach, and threatened that UHG was “walking on a very thin line.”<sup>12</sup> BlackCat described the process it had employed over many days choosing data to exfiltrate as “highly selective,” ultimately including sensitive Medicare, Tricare, CVS-Caremark, Health Net, MetLife, and numerous private insurance companies’ data, which in turn contained millions of individual medical and dental records, insurance records, payment information, telephone numbers, home and email addresses, military personnel records, and Social Security numbers, as well as over 3,000 source code files for Change Healthcare solutions.<sup>13</sup> Below is the statement that BlackCat issued regarding the cyberattack, indicating that the group has reviewed a substantial amount of confidential medical and personal identifying information:

Change Healthcare - Optum - UnitedHealth

2/28/2024, 4:19:59 PM

---

<sup>11</sup> *Id.*

<sup>12</sup> Brett Callow – X, *Twitter Post with Screenshot*, <https://twitter.com/BrettCallow/status/1762893128326111404> (Feb. 28, 2024).

<sup>13</sup> *Id.*

UnitedHealth has announced that the attack is “strictly related” to Change Healthcare only and it was initially attributed to a nation state actor.

Two lies in one sentence.

Only after threatening [sic] them to announce it was us, they started telling a different story.

It is true that the attack is centered at Change Healthcare production and corporate networks, but why is the damage extremely high? Change Healthcare production servers process extremely sensitive data to all of UnitedHealth clients that rely on Change Healthcare technology solutions. Meaning thousands of healthcare providers, insurance providers, pharmacies, etc . . .

Also, being inside a production network one can imagine the amount of critical and sensitive data that can be found.

We were able to exfiltrate to be exact more than 6 TB of highly selective data. The data relates to all Change Health clients that have sensitive data being processed by the company.

The list of affected Change Health partners that we have sensitive data for is actually huge with names such as:

- Medicare
- Tricare
- CVS-CareMark
- Loomis
- Davis Vision
- Health Net
- MetLife
- Teachers Health Trust
- Tens of insurance companies and others

Anyone with some decent critical thinking will understand what damage can be done with such intimate data on the affected clients of UnitedHealth/UnitedHealth solutions as well, beyond simple scamming/spamming.

After 8 days and Change Health have [sic] still not restored its operations and chose to play a very risky game hence our announcement today.

So for everyone, both those affected and fellow associates. [sic] to understand what is at stake our exfiltrated data includes millions of:

- active US military/navy personnel PII
- medical records
- dental records
- payments information
- Claims information
- Patients PII including Phone numbers/addresses/SSN/emails/etc ...
- 3000+ source code files for Change Health solutions (for source-code review gents out there)
- Insurance records
- many many more

UnitedHealth you are walking on a very thin line be careful you just might fall over.

PS: For all those cyber intelligence so called expert . . . we did not use ConnectWise exploit as our initial access so you should base your reports you tell people on actual facts not kiddi [sic] speculations.<sup>14</sup>

26. Screenshots, allegedly of the compromised files, have been uploaded to the dark web.<sup>15</sup> UHG later admitted that it paid a ransom to BlackCat, which many reports suggest was for

---

<sup>14</sup> *Id.*

<sup>15</sup> CNBC, *UnitedHealth paid ransom to bad actors, says patient data was compromised in Change Healthcare cyberattack*, <https://www.cnbc.com/2024/04/22/unitedhealth-paid-ransom-to-bad-actors-says-patient-data-was-compromised-in-change-healthcare-cyberattack.html> (Apr. 22, 2024).

350 Bitcoin, or approximately \$22 million.<sup>16</sup> The stolen data, apparently, is still on the dark web, because on April 7, 2024, Change received a ransom notice from a **different** group claiming to have the same data, threatening to sell it if Change did not pay a second ransom.<sup>17</sup> UHG admits that the exfiltrated data “could cover a substantial proportion of people in America.”<sup>18</sup>

**B. The System-Wide Shutdown of Change Services**

27. Soon after BlackCat activated its ransomware attack to Defendants on or around February 21, 2024, UHG “severed connectivity with Change’s data centers.”<sup>19</sup> A total shutdown continued for a month, with some systems still offline today. During the total shutdown and to a significant extent thereafter, previously-submitted claims were not paid. New claims could not be submitted. Insurance eligibility for new and existing patients could not be verified. The result was chaos for healthcare services around the country, and the consequences for both patients and providers have been devastating.

28. In a February 26, 2024 letter to Health and Human Services, the American Hospital Association (“AHA”) stated that while the full scope was “unclear,” the AHA expected impacts to be far-reaching given Change Healthcare’s national presence.<sup>20</sup> The AHA also explained how the incident has affected healthcare providers in terms of being unable to collect revenue. “[W]ithout

---

<sup>16</sup> See e.g., The Verge, *UnitedHealth CEO admits it paid \$22 million ransom to BlackCat*, <https://www.theverge.com/2024/5/1/24146693/unitedhealth-22-million-ransom-ransomware-hack-blackcat> (May 1, 2024).

<sup>17</sup> See PYMNTS, *Change Healthcare Targeted by Second Ransomware Attack*, <https://www.pymnts.com/cybersecurity/2024/change-healthcare-targeted-by-second-ransomware-attack/> (Apr. 14, 2024).

<sup>18</sup> Testimony of Andrew Witty before House Energy and Commerce Committee Subcommittee on Oversight and Investigations, *Examining the Change Healthcare Cyberattack*, [https://d1dth6e84htgma.cloudfront.net/Witty\\_Testimony\\_OI\\_Hearing\\_05\\_01\\_24\\_5ff52a2d11.pdf](https://d1dth6e84htgma.cloudfront.net/Witty_Testimony_OI_Hearing_05_01_24_5ff52a2d11.pdf) (May 1, 2024).

<sup>19</sup> *Id.*

<sup>20</sup> See American Hospital Association, *AHA Letter to HHS on Implications of Change Healthcare Cyberattack*, <https://www.aha.org/lettercomment/2024-02-26-aha-letter-hhs-implications-change-healthcare-cyberattack> (Feb. 26, 2024).

this critical revenue source, hospitals and health systems may be unable to pay salaries for clinicians and other members of the care team, acquire necessary medicines and supplies, and pay for mission critical contract work in areas such as physical security, dietary and environmental services,” the AHA stated.<sup>21</sup> “In addition, replacing previously electronic processes with manual processes will add considerable administrative costs on providers, as well as divert team members from other tasks . . . . While Change Healthcare’s systems remain disconnected, it [Change] and its parent entities benefit financially, including by accruing interest on potentially billions of dollars that belong to health care providers.”<sup>22</sup>

29. In early March, after just weeks of the outage, the AHA conducted a survey of over 1,000 providers, reporting that “74% reported direct patient care impact, including delays in authorizations for medically necessary care. . . [P]roviders are experiencing extraordinary reductions in cash flow, threatening their ability to make payroll and to acquire the medical supplies needed to provide care.”<sup>23</sup> In the same survey, 94% of hospitals reported financial impacts from the cyberattack, with more than half reporting the impact as “significant or serious.” A third of the survey respondents indicated that the attack disrupted more than half of their revenue. Another survey, of Massachusetts healthcare providers, reported costs from the outage, just in Massachusetts, from \$1 million a day for a single community hospital to \$12 million a day for a single health system.<sup>24</sup> Other analysts estimated, in mid-March, that providers were losing between

---

<sup>21</sup> *Id.*

<sup>22</sup> *Id.*

<sup>23</sup> See American Hospital Association, *AHA Urges More Congressional Action to Help Providers Affected By Change Healthcare Cyberattack*, <https://www.aha.org/lettercomment/2024-03-13-aha-urges-more-congressional-action-help-providers-affected-change-healthcare-cyberattack> (Mar. 13, 2024).

<sup>24</sup> See WBUR, *Mass. hospitals feeling fiscal pinch from Change Healthcare cyber breach*, <https://www.wbur.org/news/2024/03/12/change-healthcare-cyber-attack-massachusetts> (Mar. 12, 2024).

\$500 million and \$1 billion in daily revenue compared with 2023. The AHA sought help from the federal government, noting that “[t]he urgency of this matter grows by the day.”<sup>25</sup>

30. The federal government provided some partial relief on March 9, 2024, making available “accelerated payments” to advance funds for certain Medicare claims.<sup>26</sup> UHG also implemented a bridge loan program in early March, offering interest-free loans for a fraction of the total payments outstanding, initially with onerous rates and terms such as a five-day repayment requirement upon notice; the ability for UHG’s bank to recoup funds “immediately and without prior notification”; and a requirement that providers give UHG and its subsidiaries “access to past, current, and future claims payment data”.<sup>27</sup> Providers widely report that these programs fall far short of addressing their needs. Only after imposing a total shutdown on the industry for a full month, on or around March 22, 2024, did UHG begin to restore some of Change’s systems and to process some of the backlog in payments. By that time, a backlog of unpaid claims had accumulated—not obviously accounting for claims from the past month that providers could not even submit for payment—totaling over \$14 billion.<sup>28</sup> Restoration and repayment still are nowhere

---

<sup>25</sup> See American Hospital Association, *AHA Urges More Congressional Action to Help Providers Affected By Change Healthcare Cyberattack*, <https://www.aha.org/lettercomment/2024-03-13-aha-urges-more-congressional-action-help-providers-affected-change-healthcare-cyberattack> (Mar. 13, 2024).

<sup>26</sup> See Centers for Medicare & Medicaid Services, *Change Healthcare/Optum Payment Disruption (CHOPD) Accelerated Payments*, <https://www.cms.gov/newsroom/fact-sheets/change-healthcare/optum-payment-disruption-chopd-accelerated-payments-part-providers-and-advance> (Mar. 9, 2024).

<sup>27</sup> See Reuters, *UnitedHealth offers over \$3.3 bln in loans to providers hit by attack on unit*, <https://www.reuters.com/business/healthcare-pharmaceuticals/unitedhealth-group-has-paid-over-33-bln-care-providers-hit-by-cyberattacks-2024-03-28/> (Mar. 28, 2024); American Hospital Association, *AHA Expresses Concerns with UHG Program in Response to Cyberattack on Change Healthcare*, <https://www.aha.org/lettercomment/2024-03-04-aha-expresses-concerns-uhg-program-response-cyberattack-change-healthcare> (Mar. 4, 2024).

<sup>28</sup> *UnitedHealth Unit Will Start Processing \$14 Billion Medical Claims Backlog After Hack*, Reuters, <https://www.reuters.com/technology/cybersecurity/unitedhealth-says-several-services-handling-medical-claims-unit-change-will-go-2024-03-22/> (Mar. 22, 2024);

near complete. Providers, including Plaintiff, are still struggling to manage their businesses without a substantial portion of their earned revenues. On April 25, 2024, a coalition of 21 state attorneys general sent a letter to United demanding more meaningful action to better protect providers, pharmacies, and patients harmed by the outage, noting that providers in all 21 states were reporting “catastrophic billing and payment backlogs, and other problems stemming from the extended breakdown of Change Healthcare,” and “both Change Healthcare’s and UnitedHealth Group’s responses to the crisis have been inadequate.”<sup>29</sup> At a Senate hearing on May 1, 2024, Sen. Marsha Blackburn, R-Tenn., criticized UHG’s recovery effort saying that she has been “absolutely inundated” by providers and patients who are still struggling to get reimbursed and to get clarity about the incident.

**C. Defendants’ Prior Knowledge**

31. Nothing about ALPHV/BlackCat’s decision to test Change’s cybersecurity was extraordinary. Even putting aside the FBI’s specific advisory and recommended mitigation measures for this specific cybercriminal group (repeated and re-publicized after 2022 by other government organizations<sup>30</sup>), companies know that passwords and other login credentials are widely compromised and that they need to be prepared for cyberattacks.

32. Cybercriminals seek out PHI at a greater rate than other sources of personal information. They target the healthcare industry the most due to the treasure trove of confidential health and personal information maintained and stored by healthcare organizations. In 2023 alone,

---

<sup>29</sup> See Letter from Attorneys General, *Re: Change Healthcare Disruptions*, <https://oag.ca.gov/system/files/attachments/press-docs/4.25.24%20Letter%20to%20UnitedHealth%20Group%20CEO%20Andrew%20Witty%20re%20Change%20Healthcare%20Disruptions%5B1%5D.pdf> (Apr. 25, 2024).

<sup>30</sup> See e.g. United States Department of Justice, *Justice Department Disrupts Prolific ALPHV/Blackcat Ransomware Variant*, <https://www.justice.gov/opa/pr/justice-department-disrupts-prolific-alphvblackcat-ransomware-variant> (Dec. 19, 2023).

the FBI reported 249 ransomware attacks in the healthcare industry.<sup>31</sup> Change, in particular, is a central point of consolidation for vast amounts of PHI and PII from across the healthcare industry, and an obvious target. Indeed, UHG admits that it experiences an attempted intrusion to the company's systems on a daily basis, every 70 seconds.<sup>32</sup>

33. Cyberattacks against the healthcare industry have been common for over a decade, with the FBI warning as early as 2011 that cybercriminals targeting healthcare providers and others were “advancing their abilities to attack a system remotely” and “[o]nce a system is compromised, cyber criminals will use their accesses to obtain PII.”<sup>33</sup> The FBI again warned healthcare stakeholders in 2014 that they are the target of hackers, explaining “[t]he FBI has observed malicious actors targeting healthcare related systems, perhaps for the purpose of obtaining Protected Healthcare Information (PHI) and/or Personally Identifiable Information (PII).”<sup>34</sup>

34. The alarms have been sounding for years. In 2017, the Department of Health and Human Services released a ransomware fact sheet explaining that encryption via ransomware constitutes a “disclosure” not permitted under the HIPAA Privacy Rule.<sup>35</sup> According to an article

---

<sup>31</sup> See NPR, *Health industry struggles to recover from cyberattack on a unit of UnitedHealth*, <https://www.npr.org/sections/health-shots/2024/03/09/1237038928/health-industry-ransomware-cyberattack-change-healthcare-optum-uhc-united> (Mar. 9, 2024).

<sup>32</sup> Testimony of Andrew Witty, Chief Executive Officer, UnitedHealth Group, Before the House Energy and Commerce Committee Subcommittee on Oversight and Investigations “Examining the Change Healthcare Cyberattack,” [https://d1dth6e84htgma.cloudfront.net/Witty\\_Testimony\\_OI\\_Hearing\\_05\\_01\\_24\\_5ff52a2d11.pdf](https://d1dth6e84htgma.cloudfront.net/Witty_Testimony_OI_Hearing_05_01_24_5ff52a2d11.pdf) (May 1, 2024).

<sup>33</sup> Gordon M. Snow, FBI, *Statement before the House Financial Services Committee, Subcommittee on Financial Institutions and Consumer Credit*, <https://archives.fbi.gov/archives/news/testimony/cyber-security-threats-to-the-financial-sector> (Sept. 14, 2011).

<sup>34</sup> See Public Intelligence, *FBI Cyber Bulletin: Malicious Actors Targeting Protected Health Information*, <https://publicintelligence.net/fbi-targeting-healthcare/> (Aug. 19, 2014).

<sup>35</sup> See U.S. Department of Health and Human Services, *Fact Sheet: Ransomware and HIPAA*, <https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity/ransomware-fact-sheet/index.html> (last visited May 3, 2024).

in the HIPAA Journal posted on November 2, 2023, cybercriminals hack into healthcare networks for their “highly prized” medical records. “[T]he number of data breaches reported by HIPAA-regulated entities continues to increase every year. 2021 saw 714 data breaches of 500 or more records reported to the [HHS’ Office for Civil Rights] OCR – an 11% increase from the previous year. Almost three-quarters of those breaches were classified as hacking/IT incidents.”<sup>36</sup> This is not even the first time that the UHG family has experienced a data breach. In May 2023, United Healthcare had to notify members that protective health information may have been compromised due to a credential stuffing attack that occurred on the United Healthcare mobile app in February 2023.<sup>37</sup>

**D. Defendants’ Duty to the Class Members**

35. Defendants’ duty to Plaintiff and the Class, including their duty to use reasonable security measures and maintain an appropriate incident response plan, arose as a result of the special relationship that existed between them, on the one hand, and Plaintiff and the other Class members, on the other hand. The special relationship arose because Plaintiff and the members of the Class entrusted Defendants (or their partners who entrusted Defendants) with PHI and PII. Independent of this special relationship, Defendants also owed a common law duty to safeguard the data in their possession from foreseeable attack, to minimize the foreseeable impact of any such attack on Plaintiff and Class members. These duties arose because each of Defendants had knowledge of the threat and the resources necessary to protect their computer networks, including from ALPHV/BlackCat, but neglected to adequately invest in security measures, despite their

---

<sup>36</sup> The HIPAA Journal, *Editorial: Why Do Criminals Target Medical Records*, <https://www.hipaajournal.com/why-do-criminals-target-medical-records> (Nov. 2, 2023).

<sup>37</sup> See The HIPAA Journal, *Credential Stuffing Attack Exposed United HealthCare Member Data* <https://www.hipaajournal.com/credential-stuffing-attack-exposed-united-healthcare-member-data/> (May 2, 2023).

obligations to protect such information. Accordingly, Defendants breached their common law, statutory and other owed duties to Plaintiff and Class members.

36. Defendants' duty to use reasonable security measures also arose under HIPAA. As a healthcare company, and by handling medical patient data, Defendants are covered entities under HIPAA (45 C.F.R. § 160.103) and are required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

37. HIPAA requires covered entities to protect against reasonably anticipated threats to the security of sensitive patient health information. Defendants are subject to the rules and regulations for safeguarding electronic forms of medical information pursuant to the Health Information Technology Act ("HITECH"). *See* 42 U.S.C. § 17921, 45 C.F.R. § 160.103. HIPAA's Privacy Rule or *Standards for Privacy of Individually Identifiable Health Information* establishes national standards for the protection of health information that is kept or transferred in electronic form. HIPAA-covered entities must implement safeguards to ensure the confidentiality, integrity, and availability of PHI. Safeguards must include physical, technical, and administrative components.

38. Defendants' duty to use reasonable security measures also arose under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data by entities like Defendants. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which

established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.<sup>38</sup> The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and, have a response plan ready in the event of a breach.<sup>39</sup>

**E. Defendants' Breach of Duty**

39. Defendants breached their duty to Plaintiff and the Class at every turn, utterly failing in their obligations to implement basic industry standard cybersecurity precautions for uniquely sensitive and valuable data entrusted to them, and by worsening the impact of the data breach on the Class and on society as a whole.

40. *First*, Defendants breached their duty by inadequately protecting against criminal ingress into their systems given the known sophistication of hackers and their interest in healthcare data. Multifactor authentication ("MFA") is a very basic yet effective security measure that ordinary consumers use in the ordinary course, to access portals to information that poses a risk of harm if it falls into the wrong hands. MFA would be a basic expectation for a company handling the breadth and sensitivity of the information that flows through Change's systems. Consistent with the FBI's urging to use MFA to block entry by ALPHV/BlackCat, the Federal Cybersecurity & Infrastructure Security Agency (CISA) has also explained, in a 2022 bulletin, that MFA is

---

<sup>38</sup> Federal Trade Commission, *Protecting Personal Information: A Guide for Business*, [https://www.ftc.gov/system/files/documents/plain-language/pdf-0136\\_proteting-personal-information.pdf](https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf) (Oct. 2016).

<sup>39</sup> *Id.*

important to protect Internet-facing portals (such as Change’s Citrix portal), because “[a]dversaries are increasingly capable of guessing or harvesting passwords to gain illicit access. Password cracking techniques are becoming more sophisticated and high-powered computing is increasingly affordable. In addition, adversaries harvest credentials through phishing emails or by identifying passwords reused from other systems. MFA adds a strong protection against account takeover by greatly increasing the level of difficulty for adversaries.”<sup>40</sup> In June 2023, the U.S. Department for Health & Human Services echoed the same warnings in a newsletter issued for the healthcare industry specifically, explaining that: “Weak or non-existent authentication processes *leave your digital door open* to intrusion by malicious actors and increase the likelihood of potential compromise of sensitive information – including electronic protected health information (ePHI). Robust authentication serves as the first line of defense against malicious intrusions and attacks, yet a recent analysis of cyber breaches reported that 86% of attacks to access an organization’s Internet-facing systems (*e.g.*, web servers, email servers) used stolen or compromised credentials.”<sup>41</sup>

41. *Second*, Defendants breached their duty by allowing hackers to roam and forage within Change’s systems for nine days without detection. Monitoring a network for suspicious activity, such as unusual database access, changes in access patterns by the particular user whose credentials were employed, configuration changes to files, new software installations, and traffic from unexpected or unusual sources, are also basic cybersecurity precautions. It is extremely

---

<sup>40</sup> *Multi-Factor Authentication Fact Sheet*, <https://www.cisa.gov/sites/default/files/publications/MFA-Fact-Sheet-Jan22-508.pdf> (Jan. 2022) (emphasis added, footnote omitted).

<sup>41</sup> See US Department of Health and Human Services, *June 2023 OCR Cybersecurity Newsletter*, <https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity-newsletter-june-2023/index.html> (Jun. 2023).

unlikely that the individual whose login credentials were compromised and obtained by ALPHV/BlackCat would have a legitimate need to access, let alone download, files associated with dozens of distinct healthcare entities *and* source code files within a nine-day time span, *and* to access the systems that the hackers ultimately encrypted. Basic monitoring would also have flagged the fact that this extensive suspicious access was occurring from a new IP address or device (or several), yet it appears that not even a red flag was raised when all of these activities occurred.

42. *Third*, Defendants breached their duty by failing to wall systems off from individuals who could not conceivably need to access them; as the FBI put it, failing to “configure access controls,” and “[i]mplement network segmentation.”<sup>42</sup> This is evident in the scale and expansiveness of the exfiltrated data, as well as the fact that the hackers were able to access, via a public-facing Citrix portal, Change’s internal backup systems which would not ordinarily be required in the performance of any employee’s routine job functions.

43. *Fourth*, Defendants breached their duty by failing to control and limit the ability of a single individual to make changes to the configuration of internal systems, such as by requiring administrator credentials to install software consistent with guidance from the FBI. This is evident in the fact that, with nothing more than Citrix login credentials, hackers were able to encrypt Change’s systems and prevent Defendants from gaining access.

44. *Fifth*, Defendants breached their duty by failing to plan for a foreseeable ransomware attack, instead wreaking havoc on providers and the healthcare industry by shutting down critical services without warning. Defendants did not “[i]mplement a recovery plan to maintain and retain multiple copies of sensitive or proprietary data and servers in a physically

---

<sup>42</sup> See *supra* FBI Cyber Division, *BlackCat/ALPHV Ransomware Indicators of Compromise*, <https://www.ic3.gov/Media/News/2022/220420.pdf> (Apr. 19, 2022).

separate, segmented, secure location,” and they did not “[e]nsure copies of critical data are not accessible for modification or deletion from the system where the data resides,”<sup>43</sup> as evidenced by the fact that hackers encrypted all available copies and backups through a Citrix portal.

45. *Sixth*, Defendants breached their duty by withholding critical information from providers. Defendants failed to provide an accurate timeline for system restoration, compounding and aggravating the immense challenges healthcare providers already faced when their administrative processes were curtailed and revenues cut off. UHG did not promptly disclose the cause of the outage, the extent to which Change’s systems had been compromised, or the critically important fact, known to Defendants, that services would not be promptly restored. On the contrary, beginning in the early morning hours of February 21, 2024, UHG made a series of announcements concerning the incident on the website <https://solution-status.optum.com/> which strongly suggested that only a temporary, perhaps day-long, interruption of certain services would occur. UHG’s first announcement, posted at 2:15 a.m. ET simply stated that “some applications are currently unavailable.” Ten hours later on February 21, 2024, at 12:09 p.m. ET, UHG disclosed that it was experiencing “a network interruption due to a cyber security issue,” which, UHG stated, was “expected to last at least through the day.” On February 24, 2024, the American Hospital Association issued a security advisory notifying members and the public that “**Change Healthcare has not provided a specific timeframe for which recovery of the impacted applications is expected**” (emphasis in original).<sup>44</sup> UHG continued posting vaguely generic updates that “a cyber security issue” was expected to cause a disruption “at least through the day” for a full week, with

---

<sup>43</sup> *See id.*

<sup>44</sup> *See* American Hospital Association, *AHA Cybersecurity Advisory*, <https://www.aha.org/2024-02-24-update-unitedhealth-groups-change-healthcares-continued-cyberattack-impacting-health-care-providers> (Feb. 24, 2024).

the last such update posted February 28, 2024 at 5:58 p.m. ET., the same day that ALPHV/BlackCat publicized the nature and severity of the attack, and presumably after the hackers had informed Defendants of their intent to share information with the public.<sup>45</sup>

46. Through all of the actions and inactions above, Defendants breached their obligations to Plaintiff and Class Members and/or were otherwise negligent and reckless. On information and belief, and as discussed above, Defendants failed to meet the minimum standards under HIPAA, Section 5 of the FTC Act, and all of the following established standards in reasonable cybersecurity readiness: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC).

## **V. PLAINTIFF'S EXPERIENCE**

47. Plaintiff VIP Physicians Consulting LLC is a licensed healthcare provider serving patients in and around Fort Lauderdale, Florida.

48. Plaintiff contracted with MDLand, a cloud-based digital health services company which offers an integrated practice management system that provides healthcare providers with tools to streamline their operations.

49. MDLand, in turn, partners with Change to process insurance claims submitted by its clients, among other things. Specifically, healthcare providers such as Plaintiff submit their claims to MDLand, which in turn uses Change to process them with insurance and healthcare plans who then issue payments to providers, like Plaintiff.

---

<sup>45</sup> See Optum Solution Status, <https://solution-status.optum.com/incidents/hqpjz25fn3n7> (last visited May 3, 2024).

50. Beginning on or around February 21, 2024, when Defendants' systems were shut down in response to the cyberattack, Plaintiff could no longer submit claims through MDLand and obtain payments for those claims. During the total shutdown, Plaintiff was not paid for any claims despite continuing to treat patients. Since February 21, 2024, after changing to another clearinghouse and submitting certain claims manually, Plaintiff has received only approximately 25% of the funds that he would have received if there had been no shutdown. Plaintiff relies on the payments he receives from submitted claims to pay basic business expenses.

51. As a result of Defendants' failure to maintain the security of their computer networks, Plaintiff has had to liquidate assets, use personal credit cards, and take loans out to pay basic expenses. Plaintiff's staff resources have also been diverted to trying to resolve the cash flow problems caused by the shutdown of Defendants' computer networks.

## **VI. CLASS ACTION ALLEGATIONS**

52. Plaintiff brings this action individually and on behalf of all other persons similarly situated (the "Nationwide Class") pursuant to the Federal Rule of Civil Procedure 23(b)(2), (b)(3), and (c)(4).

53. Plaintiff proposes the following Class definition (the "Nationwide Class"), subject to amendment as appropriate:

**All healthcare providers in the United States whose use of Change Healthcare's services was disrupted by the data breach.**

54. Excluded from the Class are Defendants' officers, directors, and employees; any entity in which Defendants have a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendants. Excluded also from the Class are members of the judiciary to whom this case is assigned, their families and Members of their staff.

55. Plaintiff reserves the right to amend or modify the Class definitions or create subclasses as this case progresses.

56. ***Numerosity***. The Members of the Classes are so numerous that joinder of all of them is impracticable. Based on information and belief, the Class includes over one million licensed healthcare providers.

57. ***Commonality and Predominance***. There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

- a. Whether Defendants owed Plaintiff and Class members a legal duty to implement and maintain reasonable security procedures and practices to protect PHI and PII;
- b. Whether Defendants breached their legal duties to Plaintiff and Class members;
- c. Whether Defendants were negligent;
- d. Whether Plaintiff and Class members conferred benefits on Defendants;
- e. Whether Defendants were unjustly enriched; and
- f. Whether Plaintiff and Class Members are entitled to damages, civil penalties, punitive damages, treble damages, and/or injunctive relief.

58. ***Typicality***. Plaintiff's claims are typical of those of other Class Members because Plaintiff, like all Class members, suffered harm as a result of the data breach and shutdown of Defendants' computer networks.

59. ***Adequacy of Representation***. Plaintiff will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiff's Counsel are competent and experienced in litigating class actions.

60. ***Superiority.*** A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would also create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendants. In contrast, to conduct this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

61. ***Declaratory and Injunctive Relief Appropriate.*** Defendants have acted on grounds that apply generally to the Class as a whole, so that Class certification, injunctive relief, and corresponding declaratory relief are appropriate on a Class-wide basis.

62. ***Issue Certification.*** In the alternative, the common questions of fact and law, set forth above, are appropriate for issue certification on behalf of the proposed Class.

63. Finally, all members of the proposed Class are readily ascertainable. Defendants have access to Class Members' names and addresses affected by the data breach.

## **VII. CLAIMS FOR RELIEF**

### **COUNT I Negligence (On Behalf of Plaintiff and the Class)**

64. Plaintiff re-alleges and incorporate by reference every allegation in the preceding paragraphs as if fully set forth herein.

65. Defendants had (and continue to have) a legal duty to Plaintiff and Class members to exercise reasonable care in safeguarding and protecting confidential health and personal

identifying information on their network systems provided to them by Plaintiff and Class members. Defendants also had (and continue to have) a duty to use ordinary care in activities from which harm might be reasonably anticipated.

66. Defendants' duty to use reasonable security measures arose as a result of the special relationship that existed between them and Plaintiff and Class members, which is recognized by state and federal law, including but not limited to HIPAA. Only Defendants, however, were in a position to ensure that their computer networks were sufficient to protect against the harm to Plaintiff and the Class members that resulted from the data breach and ensuing shutdown. Plaintiff relied on Defendants to implement and maintain reasonable security procedures and practices to protect PHI and PII, and Defendants were aware of Plaintiff's reliance.

67. Defendants violated these standards and duties by failing to exercise reasonable care in safeguarding and protecting PHI and PII on their network systems by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect PHI and PII entrusted to them. It was reasonably foreseeable to Defendants that their failure to exercise reasonable care in safeguarding and protecting PHI and PII by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems would result in harm to Plaintiff and Class members.

68. Defendants, by and through their negligent actions, inaction, omissions, and want of ordinary care, unlawfully breached their duties to Plaintiff and Class members by, among other things, failing to exercise reasonable care in safeguarding and protecting their data networks and

PHI and PII within their possession, custody, and control, which resulted in the shutdown of Defendants' computer networks and disrupted Plaintiff's and Class members' businesses.

69. Defendants, by and through their negligent actions, inactions, omissions, and want of ordinary care, further breached their duties to Plaintiff and Class members by failing to design, adopt, implement, control, direct, oversee, manage, monitor and audit their processes, controls, policies, procedures, protocols, and software and hardware systems for complying with the applicable laws and safeguarding and protecting PHI and PII received from Plaintiff and Class members.

70. But for Defendants' negligent breach of the above-described duties owed to Plaintiff and Class members, Defendants would not have experienced the data breach and would not have had to shut down the Change Healthcare networks, thereby preventing Plaintiff and Class members from (i) timely receiving payments for previously submitted claims, (ii) submitting new claims for payment, and (iii) obtaining insurance authorization for patient medical treatment, among other things. The harms to Plaintiff and Class members were foreseeable given the types of services Defendants provide healthcare providers such as Plaintiff and Class members and the statutory obligations shared by all to protect computer networks and confidential PHI and PII.

71. Defendants' wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the data breach and directly resulted in the shutdown of the Change Healthcare computer networks constitute negligence.

72. As a direct and proximate result of Defendants' wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the data breach and the related shutdown, Plaintiff and Class members have suffered (and will continue to suffer) monetary losses and economic harms and seek all available damages.

**COUNT II**  
**Unjust Enrichment**  
***(On Behalf of Plaintiff and the Class)***

73. Plaintiff re-alleges and incorporate by reference every allegation in the preceding paragraphs as if fully set forth herein.

74. Plaintiff and Class members conferred benefits on Defendants in the form of payments for claims management and processing, insurance verification, authorization and medical necessity reviews, and disbursement of payments, among other things, both directly and indirectly. Defendants had knowledge of the benefits conferred by Plaintiff and Class members and appreciated such benefits. Defendants should have used, in part, the monies Plaintiff and Class members paid to them, directly and indirectly, to pay the costs of reasonable data privacy and security practices and procedures.

75. Plaintiff and Class members have suffered actual damages and harm as a result of Defendants' conduct, inactions, and omissions. Defendants should be required to disgorge into a common fund for the benefit of Plaintiff and Class members all unlawful or inequitable proceeds received from Plaintiff and Class members.

**VIII. PRAYER FOR RELIEF**

WHEREFORE, Plaintiff prays for judgment as follows:

- a) For an Order certifying this action as a Class action and appointing Plaintiff as Class Representative and his counsel as Class Counsel;
- b) For a Judgment awarding Plaintiff and Class members appropriate monetary relief, including damages, equitable relief, restitution, and disgorgement;
- c) For An Order entering injunctive and declaratory relief as appropriate under the applicable law;
- d) For an Order awarding Plaintiff and the Class pre-judgment and/or post-judgment

interest as prescribed by law;

- e) For an Order awarding reasonable attorneys' fees and costs; and
- f) For such other and further relief as this court may deem just and proper.

**IX. JURY TRIAL DEMANDED**

Plaintiff demands a trial by jury of any and all issues in this action so triable as of right.

Dated: May 3, 2024

Respectfully Submitted,



Mark P. Chalos  
mchalos@lchb.com  
Kenneth S. Byrd  
kbyrd@lchb.com  
**LIEFF CABRASER HEIMANN &  
BERNSTEIN, LLP**  
222 2nd Ave S #1640  
Nashville, TN 37201  
Tel: 615-313-9000

Jason L. Lichtman\*  
jlichtman@lchb.com  
**LIEFF CABRASER HEIMANN &  
BERNSTEIN, LLC**  
250 Hudson Street, 8th Floor  
New York, NY 10013-1314  
Tel: 212-355-9500

Michael W. Sobol\*  
msobol@lchb.com  
Melissa Gardner\*  
mgardner@lchb.com  
Michael Sheen\*  
msheen@lchb.com  
**LIEFF CABRASER HEIMANN &  
BERNSTEIN, LLC**  
275 Battery Street, 29th Floor  
San Francisco, CA 94111-3339  
Tel: 415-956-1000

*\* Pro Hac Vice Forthcoming*

*Counsel for Plaintiff and the Proposed Class*